CONFIDENTIAL

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE

Computer Security Subcommittee

IBSEC-CSS-M95
26 May 1976

COMPUTER SECURITY SUBCOMMITTEE

OF THE

DIRECTOR CENTRAL INTELLIGENCE

SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
21 May 1976

1. The ninety-fifth meeting of the Computer Security Subcommittee of the Director of Central Intelligence Security Committee was held between 0930 and 1300 hours on 21 May 1976 in Room 3F22, CIA Headquarters Building. In attendance were:

[redacted] Acting Chairman, NSA 25X1
Mr. Robert B. Cameron, Navy Member
[redacted] DIA Member 25X1
[redacted] CIA Alternate 25X1
Mr. James E. Studer, Army Member
Capt. Ron Pherigo, Air Force Member
[redacted] NSA Member 25X1
Mr. George S. Herrmann, State Member
CDR Richard Franzen, JCS Observer
[redacted] NSA Observer 25X1
[redacted] NSA Observer 25X1
LCDR Dean H. Beyer, JCS Observer
Mr. William D. Banta, DCA Observer
Mr. C. F. Letsche, DCA Observer
[redacted] DIA Observer 25X1
[redacted], NSA Observer
[redacted] NSA Observer 25X1

CONFIDENTIAL

2. The security level of the meeting was TOP SECRET SI.

3. Approval of Minutes: The minutes of the 14 May 1976 Subcommittee meeting (M-94) were approved with the following amendment: Page 2, paragraph 5, "Draft DCID 1/16" add the following to the next to last sentence "The Air Force member in cooperation with the Military departments and DIA was requested ..."

4. AUTODIN Briefing: Messrs. Banta and Letsche, DCA Communications Planners provided a briefing on AUTODIN and the AUTODIN II system.

In recent years the Department of Defense has experienced a steady growth in the number of computer-based information systems with geographically scattered terminals. The data communication requirements of these systems have usually been meet by the establishment of dedicated networks for each application system, using leased lines and in some cases, multiplexers. The current AUTODIN I, a true store and forward system, has been modified to provide a limited query/response and sequential bulk data transfer capability to accommodate some of the less stringent requirements of currently operational computer-based information systems.

AUTODIN II is designed to provide economical and reliable data communications service both for interactive timesharing and transaction-oriented systems requiring rapid response between terminals and computers, and for remote job entry and computer-to-computer data transfers requiring high transmission capacity intermittently.

AUTODIN II is based on the technology of packet-switching which was pioneered by the Defense Advanced Research Projects Agency (ARPA) with the ARPANET. Packet-switching is the modern equivalent of store and forward message-switching systems, such as AUTODIN I. Subscriber computers and terminals will be connected to their nearest AUTODIN II packet-switching node. A subscriber's data message will be broken into small units called packets, each containing up to about 250 characters (2000 bits). Each packet will contain the address of its destination, security, and community of interest information.

AUTODIN II will have security protection features that will enable it to support critical operational users including command and control and compartmented intelligence systems. Classified subscribers will be connected to the AUTODIN II packet-switch by an encrypted circuit. Each packet of data will carry with it a security-level indicator. All packets entering or leaving a packet-switch by an access circuit will be validated to ensure that they are within the security level permitted on that access circuit.

In order to provide privacy or additional security, subscribers will be identified as belonging to a particular community of interest. Such subscribers will be permitted to exchange traffic only with other subscribers within the same community of interest. The community will be identified on each packet of data. All packets entering or leaving a packet-switch by an access circuit will be validated as belonging to the community of interest for that access circuit. ADP systems managers will be responsible for identifying and controlling subscribers that belong to a community of interest. The DCA representatives stated that the current wording in the Networking mode of the draft DCID 1/16 would not impact on the consolidation efforts.

The NSA communications representatives [redacted] are of the opinion that if the draft does not address communications processors a clear statement to this effect should be stated. Such a statement has been suggested by the CIA member for inclusion in the Applicability section of the policy: "The policy is not applicable for computer hardware that is used exclusively for traditional communications message and circuit switching services that are controlled by pertinent USCSB policies and regulations". 25X1 25X1

5. The Acting Chairman requested each member to prepare in writing his views regarding the three basic problem areas with the draft DICD 1/16.

a. Definition of Intelligence which effects the scope of the paper.

b. Proposal for inclusion of the Expanded Compartmented Mode.

c. Adequacy of the Networking Mode.

6. Other Business: The next scheduled meeting will be announced at a later date.

25X1

Acting Chairman
Computer Security Subcommittee